LoadLibrary

Use fully-qualified filename to ensure that LoadLibrary() will load the correct library

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-26

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4904 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Path spoofing or confusion problem</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Indeterminate File/Path</td></tr>
<tr><td><b>Software Context</b></td><td>• Process Management</td></tr>
<tr><td><b>Location</b></td><td>• winbase.h</td></tr>
<tr><td><b>Description</b></td><td>Use care to ensure that LoadLibrary() will load the correct library.
Ensure that you specify a fully-qualified filename for the library to ensure that the correct library is always loaded.
Note: This function must not be within DllMain(), because this may create dependency loops in the DLL load order. This can result in a DLL being used before the system has executed its initialization code.
This issue is reportedly fixed in Windows XP SP1, Windows Server 2003 and newer versions of Windows.</td></tr>
<tr><td><b>APIs</b></td><td><table>
<tr><th>Function Name</th><th>Comments</th></tr>
<tr><td>LoadLibrary</td><td></td></tr>
<tr><td>LoadLibraryA</td><td>ASCII implementation</td></tr>
<tr><td>LoadLibraryW</td><td>Unicode implementation</td></tr>
<tr><td>LoadLibraryEx</td><td></td></tr>
<tr><td>LoadLibraryExA</td><td></td></tr>
<tr><td>LoadLibraryExW</td><td></td></tr>
</table></td></tr>
<tr><td><b>Method of Attack</b></td><td>An attacker could inject a Trojan horse DLL within your process by placing a "tainted" DLL in a location in the DLL search path that is found before the intended DLL.</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table>
<tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr>
</table></td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

<table>
<tr><td></td><td><table><tr><td>When a library needs to be loaded</td><td>You should consider using LoadLibraryEx with the LOAD_WITH_ALTERED_SEARCH_PATH parameter to ensure that the correct library is loaded. If you cannot use LoadLibraryEx, ensure that the lpszFileName parameter is a fully qualified filename, including the file extension. If it is not fully qualified, then the intended module can be substituted by an attacker. Also, the system will use ".dll" for the file extension if it is not specified, so "." should be appended to the end if the intended library file does not have an extension.</td><td>Effective</td></tr></table></td></tr>
<tr><td><b>Signature Details</b></td><td>HMODULE LoadLibrary(
LPCTSTR lpFileName
);
HMODULE LoadLibraryEx(
LPCTSTR lpFileName,
HANDLE hFile,
DWORD dwFlags
);</td></tr>
<tr><td><b>Examples of Incorrect Code</b></td><td><code>HMODULE hModule =</code>
<code>LoadLibrary(TEXT("someapp.dll"));</code>
<code>HMODULE hModule = LoadLibraryEx(</code>
<code>TEXT("someapp.dll"),</code>
<code>NULL,</code>
<code>0</code></td></tr>
</table>

<table>
<tr><td></td><td><code>);</code></td></tr>
<tr><td><b>Examples of Corrected Code</b></td><td><code>HMODULE hModule = LoadLibraryEx(
TEXT("C:\\The\\Right\\Directory\
\someapp.dll"),
NULL,
LOAD_WITH_ALTERED_SEARCH_PATH
);</code></td></tr>
<tr><td><b>Source Reference</b></td><td>• http://www.securityfocus.com/archive/1/353203/2004-02-09/2004-02-15/2</td></tr>
<tr><td><b>Recommended Resources</b></td><td>• MSDN reference for LoadLibrary[3]
• MSDN reference for LoadLibraryEx[4]</td></tr>
<tr><td><b>Discriminant Set</b></td><td><table>
<tr><td><b>Operating Systems</b></td><td>• Windows 98
• Windows Me
• Windows 2000
• Windows XP Home
• Windows XP Pro
• Win32</td></tr>
<tr><td><b>Languages</b></td><td>• C
• C++</td></tr>
</table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com